УДК 003.26 DOI: 10.17587/it.26.207-213

Д. Ю. Гурьянов, канд. техн. наук, доц., e-mail: guryanov.dyu@yandex.ru,
Государственный университет морского и речного флота имени адмирала С. О. Макарова, Санкт-Петербург,
А. А. Костина, науч. сотр., e-mail: to.ann@inbox.ru,
Н. А. Молдовян, д-р техн. наук, проф., e-mail: nmold@mail.ru,
Санкт-Петербургский институт информатики и автоматизации Российской академии наук, Санкт-Петербург

Постквантовый протокол бесключевого шифрования[1]

Существенный прогресс в развитии квантовых вычислителей, для которых известны полиномиальные алгоритмы факторизации целых чисел и нахождения дискретного логарифма, выдвинул на передний план проблему построения постквантовых алгоритмов и протоколов, т.е. криптосхем, которые были бы стойкими к атакам с использованием квантовых компьютеров. В работе рассматривается протокол бесключевого шифрования, стойкий к атакам с использованием квантовых компьютеров, на основе вычислительной трудности задачи дискретного логарифмирования на эллиптической кривой. В результате предложено новое построение протокола бесключевого шифрования, стойкого к квантовым атакам. Предложенный протокол отличается использованием коммутативного шифрования на эллиптической кривой и расщеплением передаваемого значения на две части, каждая из которых преобразуется на независимом локальном ключе.

Ключевые слова: *постквантовые криптосхемы, защита информации, бесключевое шифрование, коммутативное шифрование, локальные ключи, разовые ключи, стойкость, эллиптическая кривая, вычислительно сложная задача*

Введение

Криптографические методы защиты информации играют важную роль для обеспечения информационной безопасности информационно-телекоммуникационных систем [1, 2]. В частности, протоколы электронной цифровой подписи, основанные на вычислительно трудных задачах факторизации и дискретного логарифмирования, нашли широкое применение в современных информационных технологиях [3, 4], однако в случае появления в будущем квантовых компьютеров, для которых известны полиномиальные алгоритмы решения задачи дискретного логарифмирования (ЗДЛ) и задачи факторизации [5—7], потребуется заменить указанные протоколы на протоколы, основанные на вычислительно трудных задачах других типов, решение которых с использованием квантовых вычислителей будет иметь сверхполиномиальную сложность. Актуальность данной проблемы подтверждается проведением тематических конференций [8] и объявлением Национальным институтом стандартов и технологий США (НИСТ, National Institute of Standards and Technology, NIST) конкурса по разработке протоколов и алгоритмов постквантовой криптографии [9].

В качестве примитивов постквантовых криптосхем были предложены следующие вычислительные задачи: 1) поиска сопрягающего элемента в некоммутативных группах кос [10, 11] и 2) дискретного логарифмирования в скрытой циклической группе конечной некоммутативной алгебры [12—14]. Однако в первом случае имеются принципиальные трудности, обусловленные тем, что задача поиска сопрягающего элемента сводится к решению систем линейных уравнений [15]. Указанная сводимость ставит под сомнение стойкость многочисленных двухключевых криптосхем, основанных на вычислениях в группах кос [16, 17].

[1]Работа выполнена при финансовой поддержке РФФИ в рамках проекта № 18-07-00932-а.

Второй случай представляется более перспективным, однако при использовании в качестве носителей задачи дискретного логарифмирования в скрытой группе предложенных конечных некоммутативных алгебр найдены полиномиальные способы сведения этой задачи к задаче дискретного логарифмирования в конечном поле [18, 19]. Последнее определяет необходимость поиска новых типов конечных алгебр, пригодных для использования при построении постквантовых криптосхем на основе задачи дискретного логарифмирования в скрытой циклической группе.

Известные коммутативные шифры, используемые в протоколах бесключевого шифрования, основаны на вычислительной трудности задачи дискретного логарифмирования. Они также могут быть построены на основе задачи дискретного логарифмирования в скрытой циклической группе [13]. Однако в настоящее время не предложены подходящие конечные алгебры и представляет интерес рассмотрение возможности обеспечения стойкости протокола бесключевого шифрования за счет увеличения числа используемых интерактивных шагов, выполняемых абонентами сеанса секретной связи (отправителем и получателем сообщения), при использовании коммутативного шифра, основанного на вычислительной трудности задачи дискретного логарифмирования на эллиптической кривой (ЭК). Для этого может быть использован способ коммутативного шифрования на ЭК, представленный в работе [20].

В настоящей статье обсуждается построение постквантового протокола бесключевого шифрования, основанного на вычислениях на ЭК и применении разовых вспомогательных локальных ключей. Рассматриваются типовые операции на ЭК, реализация алгоритма коммутативного шифрования Похлига—Хеллмана на ЭК и его использование в стандартном трехпроходном протоколе бесключевого шифрования. Описывается предложенный постквантовый протокол бесключевого шифрования. В заключении формулируются основные выводы по выполненному исследованию.

Коммутативные шифры и протокол бесключевого шифрования

Некоторый шифр (алгоритм шифрования) E называется коммутативным, если зашифровывание некоторого сообщения M на двух разных ключах A и B приводит к формированию одного и того же шифртекста независимо от порядка использования ключей:

$$E_A(E_B(M)) = E_B(E_A(M)),$$

где A и B — произвольно выбираемые ключи, например, принадлежащие абонентам A и B соответственно. Протокол, известный как трехпроходный протокол Шамира или протокол бесключевого шифрования [21], позволяет безопасно передать секретное сообщение по открытому каналу без того, чтобы отправитель и получатель использовали заранее выполняемую процедуру согласования ключей (открытых ключей или разделяемых секретных ключей). Протокол бесключевого шифрования требует использования коммутативного шифра, который является стойким к атакам на основе известного исходного текста, в которых предполагается, что потенциальному нарушителю известно исходное сообщение и шифртекст. Последнему требованию удовлетворяет алгоритм шифрования Похлига—Хеллмана, известный как экспоненциальный шифр [21]. В нем в качестве процедуры шифрования используется операция возведения в большую натуральную степень по модулю большого простого числа p. При этом зашифровывание и расшифровывание осуществляются как возведение в степень e и d соответственно. Пара натуральных чисел (e, d), удовлетворяющих условию $ed = 1(\mathrm{mod}\ p - 1)$, представляет собой секретный ключ.

Передача секретного сообщения M, удовлетворяющего условию $M < p$, по открытому каналу связи в соответствии с протоколом бесключевого шифрования осуществляется следующим образом.

1. Алиса (отправитель сообщения) генерирует свой локальный ключ в виде пары чисел (e_A, d_A), вычисляет шифртекст $C_1 = Me_A \mathrm{mod} p$ и высылает Бобу (получателю сообщения).

2. Боб генерирует свой локальный ключ в виде пары чисел (e_B, d_B), зашифровывает шифртекст C_1 (теперь сообщение M зашифровано дважды с использованием двух различных ключей), получает шифртекст $C_2 = C_1 e_B \mathrm{mod} p = Me_A e_B \mathrm{mod} p$ и направляет C_2 Алисе.

3. Алиса расшифровывает C_2, получает шифртекст $C_3 = C_2 d_A \mathrm{mod} p = Me_A e_B d_A = Me_B \mathrm{mod} p$ (теперь сообщение M зашифровано только на ключе Боба) и направляет C_3 Бобу.

Получив шифртекст C_3, Боб легко расшифровывает сообщение: $M = C_3 d_B \mathrm{mod} p$.Потенциальный нарушитель для восстановления секретного сообщения может попытаться вычислить значе-

ние d_A из уравнения $C_3 = C_2 d_A \mathrm{mod} p$ или e_B из уравнения $C_2 = C_1 e_B \mathrm{mod} p$, однако обе последние задачи представляют собой нахождение значения дискретного логарифма по простому модулю — задачу, вычислительная сложность которой является сверхполиномиальной для современных практически реализуемых алгоритмов.

Аналогичный алгоритм коммутативного шифрования и протокол бесключевого шифрования могут быть реализованы с использованием вычислений на ЭК [20]. Для построения криптосхем используются ЭК, заданные над конечными полями [22]. В этом случае ЭК представляет собой конечные множества пар элементов (x, y) конечного поля $GF(p^s)$, где s — степень расширения ($s \geqslant 1$); p — характеристика поля ($p \geqslant 2$), удовлетворяющих уравнению третьей степени. Над таким множеством пар (x, y), называемых точками ЭК, определена операция сложения (+), обладающая свойствами коммутативности и ассоциативности. Значение суммы точек $A = (x_A, y_A)$ и $B = (x_B, y_B)$ представляет собой точку $C = (x_C, y_C)$, координаты которой вычисляются по сравнительно простым формулам, в которые входят координаты точек-операндов: $x_A, y_A, x_B, y_B \in GF(p^s)$. Вид этих формул и вид уравнения ЭК зависят от вида поля $GF(p^s)$. Например, стандарты цифровой подписи ГОСТ Р 34.10—2001 и ГОСТ Р 34.10—2012 [23] рекомендуют использование ЭК над простым полем $GF(p)$ и уравнение ЭК вида

$$y^2 = x^3 + ax + b,$$

где $a, b \in GF(p)$.

В этом случае сумма точек A и B вычисляется по формулам

$$x_c = k^2 - x_A - x_B \mathrm{mod} p,$$
$$y_c = k(x_A - x_C) - y_A \mathrm{mod} p,$$

где $k = \dfrac{y_B - y_A}{x_B - x_A} \bmod p$, если точки A и B не равны, и $k = \dfrac{3x_A + a}{2y_A} \bmod p$, если точки A и B равны. Точки $A = (x_A, y_A)$ и $-A = (x_A, -y_A)$ называются противоположными, их сумма по определению равна бесконечно удаленной точке, обозначаемой буквой O, которая считается принадлежащей ЭК. Умножение точки A на натуральное число n определяется как n-кратное сложение точки A:

$$nA = A + A + \ldots + A \ (n \text{ раз}).$$

Результат умножения любой точки ЭК на нуль определяется как точка O. Умножение на целое отрицательное число $-n$ определяется по формуле $(-n)A = n(-A)$. При задании ЭК над конечным полем она представляет собой конечную коммутативную группу. При этом групповой операцией является операция сложения точек, а нейтральным элементом — бесконечно удаленная точка O. Вычисление неизвестного $k \in GF(p)$ в уравнении $P = kG$, где P и G — известные точки ЭК, называется ЗДЛ на ЭК. Число точек на ЭК называется ее порядком и обозначается $\#E$. Известны общие методы вычисления порядка кривой по значениям p, a и b. Примеры ЭК, пригодных для построения криптосхем, приведены в стандарте [22].

В методе коммутативного шифрования на ЭК [20] используется вероятностное отображение сообщения в точку (присоединение к сообщению случайного 8-битового значения, при котором полученное значение является абсциссой некоторой точки M), лежащую на ЭК, и последующее шифрование, осуществляемое путем выполнения операции умножения сообщения-точки на число, являющееся элементом секретного ключа. Ключом является пара чисел (e, d), удовлетворяющих условию $ed = 1 \bmod \Omega$, где $\Omega = \#E$. Протокол бесключевого шифрования при использовании вычислений на ЭК описывается следующим образом.

1. Алиса (отправитель сообщения) генерирует свой локальный ключ в виде пары чисел (e_A, d_A), кодирует сообщение точкой M, вычисляет шифртекст в виде точки $C_1 = e_A M$ и высылает Бобу координаты точки C_1.

2. Боб генерирует свой локальный ключ в виде пары чисел (e_B, d_B), преобразует шифртекст C_1 в шифртекст $C_2 = e_B C_1 = e_B e_A M$ и направляет C_2 Алисе.

3. Алиса преобразует C_2 в шифртекст $C_3 = d_A C_2 = e_B M$ и направляет точку C_3 Бобу.

Получив шифртекст C_3, Боб легко расшифровывает точку-сообщение: $M = d_B C_3$. Потенциальный нарушитель для восстановления секретного сообщения может попытаться вычислить значение d_A из уравнения $C_3 = d_A C_2$ или e_B из $C_2 = e_B C_1$. Решение этих уравнений называется ЗДЛ на ЭК, которая имеет экспоненциальную сложность при правильно выбранных параметрах используемой ЭК. Однако при наличии возможности использования квантового компьютера ЗДЛ в любой циклической группе, в том числе и ЗДЛ на ЭК, имеет полиномиальную сложность. В следующем разделе представлена постквантовая версия протокола бесключевого шифрования.

Постквантовый протокол бесключевого шифрования

В качестве основной операции шифрования в описанном ниже протоколе также используется операция умножения точек ЭК, однако в процедуру шифрования дополнительно включена операция сложения с точками, представляющими собой разовые ключи. Используемая операция сложения не позволяет свести взлом протокола к решению ЗДЛ на ЭК, благодаря чему обеспечивается стойкость к атакам с использованием квантовых компьютеров. Для того чтобы внесение дополнительной шифрующей операции сохранило свойство коммутативности шифрования по ключам отправителя и получателя сообщения, в разработанном протоколе использован механизм расщепления шифруемых данных, который в рассматриваемом случае состоит в представлении шифруемой точки ЭК в виде суммы двух случайных точек и в выполнении над последними дальнейших шифрующих преобразований. Предлагаемый постквантовый протокол бесключевого шифрования описывается следующим образом.

1. Алиса (отправитель сообщения) генерирует два локальных ключа в виде пар чисел (e_{A1}, d_{A1}) и (e_{A2}, d_{A2}), кодирует сообщение точкой M (путем присоединения справа к сообщению 8 битов и получения значения абсциссы x_M), формирует пару случайных точек ЭК R_1 и R_2, таких что $R_1 + R_2 = M$. Затем преобразует точки R_1 и R_2 по формулам $C_1' = e_{A1}R_1$ и $C_1'' = e_A R_2$ и направляет точки C_1' и C_1'' Бобу.

2. Боб генерирует два своих локальных ключа в виде пар чисел (e_{B1}, d_{B1}) и (e_{B2}, d_{B2}), представляет каждую из точек C_1' и C_1'' в виде суммы двух случайных точек R_{11}, R_{12} и R_{21}, R_{22}: $R_1 = R_{11} + R_{12}$; $R_2 = R_{21} + R_{22}$. Затем генерирует две случайные точки L_1 и L_2 и преобразует точки R_{11}, R_{12}, R_{21} и R_{22} по следующим формулам:

$$C_2' = e_{B1}R_{11} + d_{B2}L_1;\ \ C_2''' = e_{B1}R_{21} + d_{B2}L_2;$$
$$C_2'' = e_{B2}R_{12} + d_{B1}L_1;\ \ \overline{C_2} = e_{B2}R_{22} + d_{B1}L_2.$$

После этого Боб направляет точки C_2', C_2'', C_2''' и $\overline{C}_2$ Алисе.

3. Алиса генерирует случайные точки N_1 и N_2 и преобразует точки C_2', C_2'', C_2''' и $\overline{C}_2$ по следующим формулам:

$$C_3' = d_{A1}C_2' + N_1;\ \ C_3''' = d_{A2}C_2''' - N_1;$$
$$C_3'' = d_{A1}C_2'' + N_2;\ \ \overline{C}_3 = d_{A2}\overline{C}_2 - N_2.$$

Затем Алиса направляет точки C_3', C_3'', C_3''' и $\overline{C}_3$ Бобу.

Боб восстанавливает точку-сообщение из точек C_3', C_3'', C_3''' и $\overline{C}_3$ путем вычисления и сложения точек S', S'', S''' и $\overline{S}$:

$$S' = d_{B1}C_3';\ S'' = d_{B2}C_3''';\ S''' = d_{B1}C_3''';\ \overline{S} = d_{B2}\overline{C}_3;$$
$$M = S' + S'' + S''' + \overline{S} = (x_M, y_M).$$

Затем он удаляет правые 8 битов в значении абсциссы x_M точки M и получает значение секретного сообщения, переданного ему Алисой.

Приведем доказательство корректности протокола. Рассмотрим следующие значения:

$$S' = d_{B1}C_3' = d_{B1}d_{A1}C_2' + d_{B1}N_1 =$$
$$= d_{B1}d_{A1}e_{B1}R_{11} + d_{B1}d_{A1}d_{B2}L_1 + d_{B1}N1 =$$
$$= d_{A1}R_{11} + d_{B1}d_{A1}d_{B2}L_1 + d_{B1}N_1;$$
$$S'' = d_{B2}C_3'' = d_{B2}d_{A1}C_2'' + d_{B2}N_2 =$$
$$= d_{B2}d_{A1}e_{B2}R_{12} - d_{B2}d_{A1}d_{B1}L_1 + d_{B2}N_2 =$$
$$= d_{A1}R_{12} - d_{B2}d_{A1}d_{B1}L_1 + d_{B2}N_2;$$
$$S''' = d_{B1}C_3''' = d_{B1}d_{A2}C_2''' - d_{B1}N_1 =$$
$$= d_{B1}d_{A2}e_{B1}R_{21} + d_{B1}d_{A2}d_{B2}L_2 - d_{B1}N_1 =$$
$$= d_{A2}R_{21} + d_{B1}d_{A2}d_{B2}L_2 - d_{B1}N_1;$$
$$\overline{S} = d_{B2}\overline{C}_3 = d_{B2}d_{A2}\overline{C}_2 - d_{B2}N_2 =$$
$$= d_{B2}d_{A2}e_{B2}R_{22} - d_{B2}d_{A2}d_{B1}L_2 - d_{B2}N_2 =$$
$$= d_{A2}R_{22} + d_{B2}d_{A2}d_{B1}L_2 - d_{B2}N_2.$$

Складывая точки S' и S'', получаем:

$$S' + S'' = d_{A1}R_{11} + d_{B1}d_{A1}d_{B2}L_1 + d_{B1}N_1 +$$
$$+ d_{A1}R_{12} - d_{B2}d_{A1}d_{B1}L_1 + d_{B2}N_2 =$$
$$= d_{A1}(R_{11} + R_{12}) + d_{B1}N_1 + d_{B2}N_2 =$$
$$= d_{A1}C_1' + d_{B1}N_1 + d_{B2}N_2 =$$
$$= d_{A1}e_{A1}R_1 + d_{B1}N_1 + d_{B2}N_2 = R_1 + d_{B1}N_1 + d_{B2}N_2.$$

Складывая точки S''' и $\overline{S}$, получаем:

$$S''' + \overline{S} = d_{A2}R_{21} + d_{B1}d_{A2}d_{B2}L_2 - d_{B1}N_1 +$$
$$+ d_{A2}R_{22} - d_{B2}d_{A2}d_{B1}L_2 - d_{B2}N_2 =$$
$$= d_{A2}(R_{21} + R_{22}) - d_{B1}N_1 - d_{B2}N_2 =$$
$$= d_{A2}C_1'' - d_{B1}N_1 - d_{B2}N_2 =$$
$$= d_{A2}e_{A2}R_2 - d_{B1}N_1 - d_{B2}N_2 = R_2 - d_{B1}N_1 - d_{B2}N_2.$$

Имеем:

$$S' + S'' + S''' + \overline{S} =$$
$$= R_1 + d_{B1}N_1 + d_{B2}N_2 + R_2 - d_{B1}N_1 - d_{B2}N_2 =$$
$$= R_1 + R_2 = M.$$

Таким образом, получатель сообщения восстанавливает точку-сообщение $M = (x_M, y_M)$,

из которой, удаляя правые 8 битов в значении абсциссы x_M, он получает значение переданного ему сообщения.

Заключение

Предложен новый вариант реализации протокола бесключевого шифрования, использующий вычислительную трудность ЗДЛ на ЭК и обеспечивающий стойкость к атакам с использованием квантового вычислителя. Последнее достигнуто благодаря тому, что в результате преобразований по перехваченным шифртекстам потенциальный нарушитель не имеет возможности в явном виде записать уравнение ЗДЛ на ЭК, поскольку дополнительно к операции умножения точки на многоразрядное число выполняется также и операция сложения со случайно выбранной точкой. При этом, для того чтобы сохранить свойство коммутативности преобразований, выполняемых отправителем сообщения и получателем, случайные точки-слагаемые входят в преобразования дважды, причем с противоположными знаками. Для того чтобы потенциальный нарушитель не смог воспользоваться последним, преобразуемые точки "расщепляются" в сумму двух точек, каждая из которых преобразуется на различных локальных ключах текущего пользователя. Такое расщепление выполняется в ходе выполнения протокола один раз отправителем. Другая сторона (получатель), получая два шифртекста, выполняет расщепление каждого из них, поэтому на первом шаге шифртекст передается в виде двух точек ЭК, а на втором и третьем — в виде четырех точек.

Производительность предложенного протокола определяется, главным образом, вычислительной сложностью операции умножения точки ЭК на многоразрядное число аналогично реализации на ЭК стандартного трехпроходного протокола бесключевого шифрования, хотя первый из протоколов требует выполнения в два раза большего числа таких операций. Однако снижение производительности в два раза является приемлемой издержкой для обеспечения стойкости к квантовым атакам. Программная и аппаратная реализации операции умножения точки ЭК являются хорошо апробированными. В целом с практической точки зрения предложенный постквантовый протокол обладает достаточной производительностью при программной и аппаратной его реализации.

Следует отметить, что протоколы бесключевого шифрования обеспечивают высокий уровень секретности к атакам пассивного нарушителя. Для обеспечения защиты от активных атак требуется встроить механизм взаимной аутентификации участников протокола. Например, это может быть сделано с использованием коротких ключей малого размера (от 16 до 56 бит) по аналогии с криптосхемой [24].

Постквантовый протокол бесключевого шифрования может быть построен по аналогии с предложенной криптосхемой также и при использовании вычислений в конечных полях, например, в простых полях $GF(p)$ или двоичных полях $GF(2^s)$. При этом реализация протокола над полями $GF(2^s)$ со степенью расширения, равной степени Мерсенна, представляет особый интерес, поскольку мультипликативная группа таких полей имеет порядок, равный простому числу Мерсенна [25]. Предложенная схема построения постквантового протокола может быть реализована и с использованием вычислительной трудности скрытой ЗДЛ [13]. Детальное рассмотрение указанных вариантов реализации протокола представляет самостоятельный интерес.

Список литературы

1. **Yiteng Feng, Guomin Yang, Joseph K. Liu.** A new public remote integrity checking scheme with user and data privacy // International Journal of Applied Cryptography. 2017. Vol. 3, N. 3. P. 196—209.
2. **Sirwan A., Majeed N.** New Algorithm for Wireless Network Communication Security // International Journal on Cryptography and Information Security. 2016. Vol. 6, N. 3/4. P. 1—8.
3. **Chiou S. Y.** Novel Digital Signature Schemes based on Factoring and Discrete Logarithms // International Journal of Security and Its Applications. 2016. Vol. 10, N. 3. P. 295—310.
4. **Poulakis D.** A variant of Digital Signature Algorithm // Designs, Codes and Cryptography. 2009. Vol. 51, N. 1. P. 99—104.
5. **Yan S. Y.** Quantum Computational Number Theory. Springer, 2015. 252 p.
6. **Yan S. Y.** Quantum Attacks on Public-Key Cryptosystems. Springer, 2014. 207 p.
7. **Smolin J. A., Smith G., Vargo A.** Oversimplifying quantum factoring // Nature. 2013. Vol. 499, N. 7457. P. 163—165.
8. **Proceedings** of the 7th International Workshop on Post-Quantum Cryptography, PQCrypto 2016. Fukuoka, Japan, February 24—26, 2016 // Lecture Notes in Computer Science (LNCS) series. Springer, 2016. Vol. 9606. 270 p.
9. **Federal** Register:: Announcing Request for Nominations for Public-Key Post-Quantum Cryptographic Algorithms // Federal Register. The Daily journal of the United States Government. URL: https://www.gpo.gov/fdsys/pkg/FR-2016-12-20/pdf/2016-30615.pdf (дата обращения 07.11.2019).
10. **Verma G. K.** A Proxy Blind Signature Scheme over Braid Groups // International Journal of Network Security. 2009. V.9, N. 3. P. 214–217.
11. **Hiranvanichakorn P.** Provably Authenticated Group Key Agreement based on Braid Groups — The Dynamic Case // International Journal of Network Security. 2017. V. 19, N. 4. P. 517—527.
12. **Sakalauskas E., Tvarijonas P., Raulynaitis A.** Key Agreement Protocol (KAP) Using Conjugacy and Discrete Logarithm

Problems in Group Representation Level // Informatica. 2007. Vol. 18, N. 1. P. 115—124.

13. **Moldovyan D. N.** Non-Commutative Finite Groups as Primitive of Public-Key Cryptoschemes // Quasigroups and Related Systems. 2010. Vol. 18. P. 165—176.

14. **Kuzmin A. S., Markov V. T., Mikhalev A. A., Mikhalev A. V., Nechaev A. A.** Cryptographic Algorithms on Groups and Algebras // Journal of Mathematical Sciences. 2017. Vol. 223, N. 5. P. 629—641.

15. **Myasnikov A., Shpilrain V., Ushakov A.** A Practical Attack on a Braid Group Based Cryptographic Protocol // In: Advances in Cryptology — CRYPTO'05 / Lecture Notes in Computer Science. Springer-Verlag, 2005. Vol. 3621. P. 86—96.

16. **Chaturvedi A., Lal S.** An Authenticated Key Agreement Protocol Using Conjugacy Problem in Braid Groups // International Journal of Network Security. 2008. V.6, N. 2. P. 181—184.

17. **Verma G. K.** Probable Security Proof of a Blind Signature Scheme over Braid Groups // International Journal of Network Security. 2011. Vol. 12, N. 2. P. 118—120.

18. **Кузьмин А. С., Марков В. Т., Михалев А. А., Михалев А. В., Нечаев А. А.** Криптографические алгоритмы на группах и алгебрах // Фундаментальная и прикладная математика. 2015. Т. 20, № 1. С. 205—222.

19. **Глухов М. М.** К анализу некоторых систем открытого распределения ключей, основанных на неабелевых группах // Математические вопросы криптографии. 2010. Т. 1, № 4. С. 5—22.

20. **Молдовян Н. А., Рыжков А. В.** Способ коммутативного шифрования на основе вероятностного кодирования // Вопросы защиты информации. 2013. № 3. С. 3—10.

21. **Menezes A. J., Van Oorschot P. C., Vanstone S. A.** Handbook of Applied Cryptography. Boca Raton, FL: CRC Press, 1997. 780 p.

22. **National** Institute of Standards and Technology, Digital Signature Standard, FIPS Publication 186-3, 2009.

23. **Информационная** технология. Криптографическая защита информации. Процессы формирования и проверки электронной цифровой подписи. Национальный стандарт Российской Федерации ГОСТ Р 34.10—2012. М., Стандартинформ. 32 с.

24. **Молдовян Н. А., Горячев А. А., Муравьев А. В.** Протокол стойкого шифрования по ключу малого размера // Вопросы защиты информации. 2015. № 1. С. 3—8.

25. **Moldovyan N. A., Moldovyan A. A., Berezin A. N.** On Using Mersenne Primes in Designing Cryptoschemes // Int. Journal of Network Security. 2016. Vol. 18, N. 2. P. 369—373.

D. Yu. Guryanov, PhD, Tech., Associate Professor, e-mail: guryanov.dyu@yandex.ru,
Admiral Makarov State University Maritime and Inland Shipping,
Saint-Petersburg, 198035, Russian Federation,
A. A. Kostina, Research Fellow of Laboratory of Information Systems Security, e-mail: to.ann@inbox.ru,
N. A. Moldovyan, Dr. Sc., Tech., Professor, Chief Researcher of Laboratory
of Information Systems Security, e-mail: nmold@mail.ru,
St. Petersburg Institute for Informatics and Automation of the Russian Academy of Sciences,
Saint-Petersburg, 199178, Russian Federation

Post-Quantum Protocol for No-Key Encryption

The most widely used cryptoschemes with public key are based on computational difficulty of the factorization problem and on the discrete logarithm problem. The known no-key protocols are base on the second problem. Significant progress in the development of quantum computers for which there is known polynomial algorithm for integer factoring and for finding discrete logarithm have put forward problem of construction of the post-quantum algorithms and protocols, i.e. cryptoschemes that are secure to potential attacks using quantum computers. The paper considers a protocol no-key encryption, which is secure to attacks using quantum computers, on the base of the discrete logarithm on elliptic curve. As a method, at the first step of the protocol the sender divides the sent message into two values and encrypts each of them on independent local keys. At the second step analogous procedure is performed by the receiver over each of two received ciphertexts. As a result, it is proposed a new design of the no-key encryption protocol based on commutative encryption function, which is secure against quantum attacks. The proposed protocol is characterized in using commutative encryption on elliptic curve and dividing the encrypted value into two parts followed by encryption of each part using independent local key. The proposed protocol possesses sufficiently high performance and suites well for software and hardware implementations.

Keywords: *post-quantum cryptoschemes, information protection, no-key encryption, commutative encryption, local keys, single-use keys, security, elliptic curve, computationally difficult problem*

DOI: 10.17587/it.26.207-213

References

1. **Yiteng Feng, Guomin Yang, Joseph K. Liu.** A new public remote integrity checking scheme with user and data privacy, *International Journal of Applied Cryptography*, 2017, vol. 3, no. 3, pp. 196—209.

2. **Sirwan A., Majeed N.** New Algorithm for Wireless Network Communication Security, *International Journal on Cryptography and Information Security,* 2016, vol. 6, no. 3/4, pp. 1—8.

3. **Chiou S. Y.** Novel Digital Signature Schemes based on Factoring and Discrete Logarithms, *International Journal of Security and Its Applications,* 2016, vol. 10, no. 3, pp. 295—310.

4. **Poulakis D.** A variant of Digital Signature Algorithm, *Designs, Codes and Cryptography*, 2009, vol. 51, no. 1, pp. 99—104.

5. **Yan S. Y.** Quantum Computational Number Theory, Springer, 2015, 252 p.

6. **Yan S. Y.** Quantum Attacks on Public-Key Cryptosystems, Springer, 2014, 207 p.

7. **Smolin J. A., Smith G., Vargo A.** Oversimplifying quantum factoring, *Nature*, 2013, vol. 499, no. 7457, pp. 163—165.

8. **Proceedings** of the 7th International Workshop on Post-Quantum Cryptography, PQCrypto 2016. Fukuoka, Japan, Feb-

ruary 24—26, 2016, *Lecture Notes in Computer Science (LNCS) series*, Springer, 2016, vol. 9606, 270 p.

9. **Federal** Register:: Announcing Request for Nominations for Public-Key Post-Quantum Cryptographic Algorithms, *Federal Register. The Daily journal of the United States Government,* available at: https://www.gpo.gov/fdsys/pkg/FR-2016-12-20/pdf/2016-30615.pdf (date of the application 07.11.2019).

10. **Verma G. K.** A Proxy Blind Signature Scheme over Braid Groups, *International Journal of Network Security*, 2009, vol. 9, no. 3, pp. 214—217.

11. **Hiranvanichakorn P.** Provably Authenticated Group Key Agreement based on Braid Groups — The Dynamic Case, *International Journal of Network Security*, 2017, vol. 19, no. 4, pp. 517—527.

12. **Sakalauskas E., Tvarijonas P., Raulynaitis A.** Key Agreement Protocol (KAP) Using Conjugacy and Discrete Logarithm Problems in Group Representation Level, *Informatica*, 2007, vol. 18, no. 1, pp. 115—124.

13. **Moldovyan D. N.** Non-Commutative Finite Groups as Primitive of Public-Key Cryptoschemes, *Quasigroups and Related Systems*, 2010, vol. 18, pp. 165—176.

14. **Kuzmin A. S., Markov V. T., Mikhalev A. A., Mikhalev A. V., Nechaev A. A.** Cryptographic Algorithms on Groups and Algebras, *Journal of Mathematical Sciences*, 2017, vol. 223, no. 5, pp. 629—641.

15. **Myasnikov A., Shpilrain V., Ushakov A.** A Practical Attack on a Braid Group Based Cryptographic Protocol, *In: Advances in Cryptology — CRYPTO'05 / Lecture Notes in Computer Science*, Springer-Verlag, 2005, vol. 3621, pp. 86—96.

16. **Chaturvedi A., Lal S.** An Authenticated Key Agreement Protocol Using Conjugacy Problem in Braid Groups, *International Journal of Network Security*, 2008, vol. 6, no. 2, pp. 181—184.

17. **Verma G. K.** Probable Security Proof of a Blind Signature Scheme over Braid Groups, *International Journal of Network Security*, 2011, vol. 12, no. 2, pp. 118—120.

18. **Kuzmin A. S., Markov V. T., Mikhalev A. A., Mikhalev A. V., Nechaev A. A.** Cryptographic Algorithms on Groups and Algebras, *Fundamentalinaya i Prikladnaya Matematika*, 2015, vol. 20, no. 1, pp. 205—222 (in Russian).

19. **Glukhov M. M.** On analysis of some public key distribution systems based on non-abelian groups, *Matematicheskie Voprosy Kriptografii*, 2010, vol. 1, no. 4, pp. 5—22 (in Russian).

20. **Moldovyan N. A., Rizkov A. V.** Method for Commutative Encryption Based on Probabilistic Coding, *Information Security Issues*, 2013, vol. 3, pp. 3—10 (in Russian).

21. **Menezes A. J., Van Oorschot P. C., Vanstone S. A.** Handbook of Applied Cryptography, Boca Raton, FL, CRC Press, 1997, 780 p.

22. **National** Institute of Standards and Technology, Digital Signature Standard, FIPS Publication 186-3, 2009.

23. **Information** technology. Cryptographic protection of the information. Processes for generation and verification of the electronic digital signature. National standard of Russian Federation GOST R 34.10-2012, Moscow, Standartinform, 32 p. (in Russian).

24. **Moldovyan N. A., Goryachev A. A., Muravev A. V.** Protocol Strong Encryption Employing Key of Small Size, *Information security issues*, 2015, vol. 1, pp. 3—8 (in Russian).

25. **Moldovyan N. A., Moldovyan A. A., Berezin A. N.** On Using Mersenne Primes in Designing Cryptoschemes, *Int. Journal of Network Security*, 2016, vol. 18, no. 2, pp. 369—373.

УДК 004.89 DOI: 10.17587/it.26.213-221

В. И. Васильев, д-р техн. наук, проф., e-mail: vasilyev@ugatu.ac.ru,
А. М. Вульфин, канд. техн. наук, доц., e-mail: vulfin.alexey@gmail.com,
М. Б. Гузаиров, д-р техн. наук, проф., e-mail: guzairov@ugatu.su,
В. М. Картак, д-р физ.-мат. наук, доц., e-mail: kvmail@mail.ru,
Л. Р. Черняховская, д-р техн. наук, проф., e-mail: lrchern@yandex.ru,
Уфимский государственный авиационный технический университет

Оценка рисков кибербезопасности АСУ ТП промышленных объектов на основе вложенных нечетких когнитивных карт[1]

Рассмотрены методические аспекты количественной оценки рисков кибербезопасности АСУ ТП промышленных предприятий. В качестве базового подхода предлагается использование риск-ориентированного подхода, заложенного в основу стандартов серии ГОСТ Р 62443. Применение вложенных нечетких серых когнитивных карт при этом обеспечивает возможность получить более обоснованные и достоверные количественные оценки показателей рисков кибербезопасности АСУ ТП. Рассмотрен пример применения данной технологии для оценки защищенности телеметрической информации о состоянии бортовых авиационных систем.

Ключевые слова: *кибербезопасность, оценка рисков, когнитивное моделирование, нечеткая серая когнитивная карта*

Введение

В последние годы в нашу жизнь все более прочно входят новые термины и понятия: "цифровизация экономики", "промышленный интернет вещей", "киберфизические системы", "киберпространство", "кибербезопасность". Неизбежным следствием промышленной революции 4.0 при этом является не только ожидаемый рост эффективности, качества и производительности производства, но и все

[1]Исследование выполнено при финансовой поддержке РФФИ в рамках научного проекта № 18-00-00238 КОМФИ.